Listing of the Claims

This listing of claims will replace all prior versions, and listings, of claims in this application.

1. (Previously presented) A method for securely installing an applet on a computer system having a data storage and a secure processor, comprising:

receiving an applet in the data storage;

with the secure processor, determining from at least a portion of the applet whether the applet is capable of being executed by the secure processor, wherein the portion of the applet includes at least one of a security meta-data portion, a resource meta-data portion, and a meta-data signature portion; and

installing the applet on the secure processor if the secure processor is capable of executing the applet.

2. (Original) The method according to claim 1, wherein the applet is stored in a non-secure storage.

3. (Previously presented) The method according to claim 2, wherein the applet further comprises: an executable portion.

4. (Original) The method according to claim 3, wherein the applet further comprises a certificate portion.

5. (Canceled)

6. (Previously presented) The method according to claim 3, wherein the resource meta-data portion is adapted to designate resources comprising at least one of:

a biometric sensor;

a secure output;

a keyboard;

a personal identification number entry device;

a global positioning system input;

a magnetic stripe card reader;

a secure storage area;

a performance metrics,

an algorithm implementing specific cryptographic algorithms; and

at least one smart card slot.

7. (Previously presented) The method according to claim 3, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises loading the meta-data portion of the applet into a secure storage area in the secure processor.

8. (Original) The method according to claim 7, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises cryptographically verifying the security meta-data portion and the resource meta-data portion of the meta-data portion of the applet against the signature portion of the meta-data portion of the applet.

9. (Original) The method according to claim 7, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises verifying that a secure processor security requirement of the security meta-data portion of the applet is met or exceeded by a secure processor security rating of the secure processor.

10. (Original) The method according to claim 9, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises:

determining that the secure processor security requirement of the security meta-data portion of the applet is not met or exceeded by a secure processor security rating of the secure processor; and

suggesting the use of a second applet that may have a second secure processor security requirement that is met or exceeded by the secure processor security rating of the secure processor.

11. (Original) The method according to claim 10, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises charging a premium for the use of the second applet.

12. (Original) The method according to claim 7, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises verifying that the secure processor is capable of supplying resources designated in the resource meta-data portion of the meta-data portion of the applet.

13. (Original) The method according to claim 12, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises:

determining that the secure processor is not capable of supplying at least one of the resources designated in the resource meta-data portion of the meta-data portion of the applet; and

suggesting the use of a second applet that may designate only resources that the secure processor is capable of supplying.

14. (Original) The method according to claim 3, wherein the executable portion further comprises:

an encrypted executable; and

an unencrypted executable signature.

15. (Original) The method according to claim 14, wherein the step of installing the applet on the secure processor further comprises storing the executable portion of the applet in the secure storage area.

16. (Original) The method according to claim 15, wherein the step of installing the applet on the secure processor further comprises:

requesting a decryption key for the encrypted executable portion of the applet;

receiving the decryption key; and

decrypting the encrypted executable portion into an unencrypted executable portion using the decryption key.

17. (Original) The method according to claim 16, wherein the step of installing the applet on the secure processor further comprises verifying the unencrypted executable portion against the unencrypted executable signature.

18. (Original) The method according to claim 16, wherein the step of installing the applet on the secure processor further comprises verifying the unencrypted executable portion prepended with an applet serial number against the unencrypted executable signature.

19. (Original) The method according to claim 17, wherein the step of installing the applet on the secure processor further comprises binding the unencrypted executable portion to the secure processor.

20. (Original) The method according to claim 17, wherein the step of installing the applet on the secure processor further comprises:

encrypting the unencrypted executable portion to an encrypted executable;

storing the encrypted executable in the non-secure storage; and

storing the encrypted executable's decryption key in the secure storage area.

21. (Original) The method according to claim 1, wherein the computer system further comprises a non-secure processor.

22. (Original) A method for securely installing an applet on a computer system having a data storage and a secure processor, comprises:

receiving an applet in a non-secure data storage, said applet comprises:

a meta-data portion, said meta-data portion comprises:

a security meta-data portion;

a resource meta-data portion which designates any resources required by the applet for execution; and

a meta-data signature portion; and

an executable portion;

determining whether the applet is capable of being executed by a secure processor based at least in part on the security meta-data portion and the resource meta-data portion of the applet, comprises:

verifying that a secure processor security requirement of the security meta-data portion of the applet is met or exceeded by a secure processor security rating of the secure processor; and

verifying that the secure processor is capable of supplying the resources designated in the resource meta-data portion of the meta-data portion of the applet; and

installing the applet on the secure processor if the secure processor is capable of executing the applet.

23. (Original) The method according to claim 22, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises verifying the security meta-data portion and the resource meta-data portion of the meta-data portion of the applet against the signature portion of the meta-data portion of the applet.

24. (Original) The method according to claim 23, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises:

determining that the secure processor security requirement of the security meta-data portion of the applet is not met or exceeded by a secure processor security rating of the secure processor; and

suggesting the use of a second applet that may have a second secure processor security requirement that is met or exceeded by the secure processor security rating of the secure processor.

25. (Original) The method according to claim 24, wherein the step of determining whether the applet is capable of being executed by the secure processor further comprises charging a premium for the use of the second applet.

26. (Original) The method according to claim 22, wherein the step of installing the applet on the secure processor further comprises storing the executable portion of the applet in the secure storage area.

27. (Original) The method according to claim 26, wherein the step of installing the applet on the secure processor further comprises:

requesting a decryption key for the encrypted executable portion of the applet;

receiving the decryption key; and

decrypting the encrypted executable portion into an unencrypted executable portion using the decryption key.

28. (Original) The method according to claim 26, wherein the step of installing the applet on the secure processor further comprises:

decrypting the encrypted executable portion into an unencrypted executable

portion using a decryption key; and

binding the unencrypted executable portion to the secure processor.

29. (Original) The method according to claim 28, wherein the step of installing the applet on the secure processor further comprises:

encrypting the unencrypted executable portion to an encrypted executable;

storing the encrypted executable in the non-secure storage; and

storing the encrypted executable's decryption key in the secure storage area.

30. (Original) A method for providing a list of alternative applets for a first applet which could not be installed in a computer having at least one resource and having a secure processor which is associated with a security rating, comprising:

receiving a request from a secure processor for a list of alternative applets;

the request comprising:

an applet serial number which identifies a first applet;

an identifier which identifies the secure processor;

a first indicator which identifies a security rating of the secure processor; and

a second indicator which identifies the at least one resource of the computer;

creating the list of alternative applets from the plurality of applets based at least in part on the first indicator and the second indicator; and

transmitting the list of alternative applets to the computer.

31. (Original) The method according to claim 30, further comprises:

installing an alternative applet from the list of alternative applets; and

charging a premium for installing the alternative applet.

32. (Original) The method according to claim 30, wherein the identifier identifies the secure processor uniquely.

33. (Previously presented) A secure applet execution system, comprising:

a data storage element storing an applet received by the secure applet execution system; and

a secure processor determining from at least a portion of the applet whether the applet is capable of being executed by the secure processor, wherein the portion of the applet includes at least one of a security meta-data portion, a resource meta-data portion, and a meta-data signature portion, and installing the applet on the secure processor if the secure processor is capable of executing the applet.

34. (Original) The secure applet execution system according to claim 33, wherein the applet further comprises:

a meta-data portion; and

an executable portion.

35. (Original) The secure applet execution system according to claim 34, wherein the applet further comprises a certificate portion.

36. (Original) The secure applet execution system according to claim 35, wherein the meta-data portion further comprises:

a security meta-data portion;

a resource meta-data portion which designates any resources required by the applet for execution; and

a meta-data signature portion.

37. (Original) A secure applet execution system, comprising:

a non-secure data storage element storing an applet received by the secure applet execution system;

said applet comprising:

a meta-data portion; and

an executable portion;

said meta-data portion, comprising:

a security meta-data portion;

a resource meta-data portion which designates any resources required by the applet for execution; and

a meta-data signature portion; and

a secure processor determining from at least a portion of the applet whether the applet is capable of being executed by the secure processor, and installing the applet on the secure processor if the secure processor is capable of executing the applet.

38. (Original) A secure applet configured to include a cryptographically secure executable, comprising:

a meta-data portion, said meta-data portion including:

a security meta-data portion;

a resource meta-data portion; and

a meta-data signature portion;

an executable portion, said encrypted executable portion including:

an encrypted executable portion; and

an unencrypted executable signature portion; and

a certificate portion.

39. (Original) The secure applet according to claim 38, wherein said security meta-data portion comprises information describing security requirements necessary for the decryption and execution of the encrypted executable portion.

40. (Original) The secure applet according to claim 38, wherein the resource meta-data portion comprises information describing resources necessary to execute the encrypted executable portion.

41. (Original) The secure applet according to claim 38, wherein the resource meta-data portion comprises an applet serial number.

42. (Original) The secure applet according to claim 41, wherein the unencrypted signature portion comprises information adapted to verify whether the encrypted executable portion, when decrypted and prepended by the applet serial number, has been modified in any way.

43. (Original) The secure applet according to claim 38, wherein the meta-data signature portion comprises information adapted to verify whether the security meta-data portion and the resource meta-data portion have been modified in any way.